IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	)	
	)	Confirmation No: 2520
Adrian Patrick Kent, *et al.*	)	
	)	Group Art Unit: 2137
Serial No.: 10/627,158	)	
	)	Examiner: Popham, Jeffrey D.
Filed: July 25, 2003	)	
	)	Atty. Docket No.: 200206289-1
For: Improvements Relating to Quantum Cryptography	)	

REPLY BRIEF RESPONSIVE TO EXAMINER'S ANSWER

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

The Examiner's Answer mailed April 16, 2008 has been carefully considered. In response thereto, please consider the following remarks.

AUTHORIZATION TO DEBIT ACCOUNT

It is not believed that extensions of time or fees for net addition of claims are required, beyond those which may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to deposit account no. 08-2025.

REMARKS

The Examiner has provided in the Examiner's Answer various responses to arguments contained in Applicants' Appeal Brief. Although the Examiner's Answer has added some additional remarks in response to Applicants' arguments, the substance of the rejections and the Examiner's positions have not changed. Accordingly, Applicants stand behind the arguments set forth in the Appeal Brief. In addition, Applicants address selected responses in the following.

Applicants respectfully submit that *Bennett* in view of *Sych* fails to teach or suggest at least "transmitting to the recipient composition information describing a subset of the plurality of random quantum states; analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states; establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar; [and] deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset," as recited in claim 1, as an example

To attempt to refute this contention, the Examiner in explaining the disclosure of *Bennett* states that the "communicating parties, Alice (the sender) and Bob (the receiver) communicate information regarding which measurements were made in the correct bases by Bob, discarding those results that were measured with wrong bases."

Page 19 of Examiner's Answer. Diversely, the claimed subject matter does not have the underlying requirement of making known which photons had correctly measured bases and then using these correctly measured photons to become a key. Rather, claim 1, as an example, describes that a subset of transmitted photons are used to derive statistical distributions describing transmitted and received quantum states, where the subset is then discarded, and from the remaining quantum states, a first binary string is derived from the transmitted quantum states and a second binary string is derived from the received quantum states (which were not in the subset of quantum states used to derive the statistical distributions). The Examiner also points to the footnote on page 7 of *Bennett* which refers to a reconciliation process for comparing respective keys. Applicants note that the keys being compared are the result of the bases that were made known to have been correctly measured by a sender, which differs from the claimed subject matter.

Further, *Sych* describes "that secure quantum information channel is used first to transfer a secret key from Alice to Bob, which is then used to encrypt messages transmitted via an insecure classical channel." Page 4. *Sych* discloses: "When transmission of the message is completed, Alice and Bob disclose part of the measurement results transmitting them over an insecure classical channel in order to determine the mutual probability distribution, which is then used for calculation of an average amount of transmitted information per an elementary step of the QC-protocol. After that, disclosed results are discarded and not used for further generation of a secret key. If the security condition (8) is fulfilled, Alice and Bob decide that the secret key

transfer is completed, otherwise the transmitted key is not used." Page 5. Accordingly, *Sych* individually or in combination with *Bennett* does not disclose a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the subset of measured quantum states. Rather, *Sych* describes a single mutual probability distribution indicating an amount of information Bob (receiver) receives from Alice (sender). Pages 4-5.

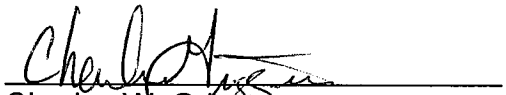
For at least these reasons, *Bennett* in view of *Sych* fails to teach or suggest at least "transmitting to the recipient composition information describing a subset of the plurality of random quantum states; analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states; establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar; [and] deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset," as recited in claim 1.

Using similar reasoning, the cited art also does not teach or suggest the subject matter of remaining claims 2-49. Therefore, for the reasons presented herein and the reasons earlier presented in the Appeal Brief, the cited references are deficient in disclosing claimed features, and the arguments set forth in the Appeal Brief still stand. The rejection of the pending claims should be overturned.

Conclusion

In summary, it is Applicants' position that Applicants' claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicants' pending claims.

Respectfully submitted,

By: 

Charles W. Griggers
Registration No. 47,283